SOFTWARE ENGINEERING

PROFESSIONAL ETHICS

TABLE OF CONTENTS

[EXECUTIVE SUMMARY 2](#_TOC_250005)

[INTRODUCTION 2](#_TOC_250004)

[LEGAL ANALYSIS 3](#_TOC_250003)

BRITISH COLUMBIA LAW 3

CANADA LAW 3

[MORAL AND ETHICAL ANALYSIS 4](#_TOC_250002)

PRINCIPLE 1: PUBLIC 5

PRINCIPLE 2: CLIENT AND EMPLOYER 5

PRINCIPLE 3: PRODUCT 6

PRINCIPLE 4: JUDGEMENT 7

PRINCIPLE 5: MANAGEMENT 7

PRINCIPLE 6: PROFESSION 7

PRINCIPLE 7: COLLEAGUES 8

PRINCIPLE 8: SELF 8

[CONCLUSION 9](#_TOC_250001)

[BIBLIOGRAPHY 10](#_TOC_250000)

# EXECUTIVE SUMMARY

In recent years, the collection and analysis of big data have become ubiquitous in modern system design. Although this approach has numerous advantages, it also presents challenging moral and legal problems regarding secrecy and privacy. We will specifically address the issue of mining and selling aggregate data in this study because it has become prevalent among businesses that offer web hosting for e-commerce websites. We will analyze the ethical and legal implications of this practice considering Canadian and British Columbian legislative framework. We will demonstrate that while mining and selling aggregate information is technically legal, it is not always morally right. We shall conclude that software engineers have a responsibility to design systems that protect users' privacy and security and must adhere to the ACM/IEEE Software Engineering Code of Ethics.

# INTRODUCTION

Big data collecting and analysis are now common procedures in contemporary system design. Big data can be gathered, categorized, and analyzed to help businesses learn more about their customers than they could from just their own activities. Although this approach has numerous advantages, it also presents some serious moral and legal problems regarding secrecy and privacy. One such problem is the widespread practise of mining and selling aggregate information among businesses that offer web hosting for e-commerce websites.

In the process of mining and selling aggregate information, transactional data from online retailers is gathered, then examined to develop a unique profile of client trends. Then, this knowledge is offered to other businesses so that they can utilize it to enhance their marketing approaches or acquire a competitive edge. Although mining and selling aggregate data is legally lawful, it poses numerous moral and ethical issues around user consent, privacy, and secrecy.

# LEGAL ANALYSIS

**BRITISH COLUMBIA LAW**

Personal information collection, use, and disclosure are all regulated by law in British Columbia. Private sector organizations in British Columbia are subject to the Personal Information Protection Act (PIPA), which places restrictions on how they can acquire, use, and disclose personal information. PIPA mandates that businesses get consent before collecting, using, or disclosing any personal information, and that they use and disclose that information only as needed to achieve the goals for which it was originally gathered.

However, PIPA does not explicitly prohibit the collection and sale of aggregate information, which makes it difficult to regulate this practice. In accordance with the rules on the use of aggregate data published by the Information and Privacy Commissioner of British Columbia, businesses must take the necessary precautions to secure personal information when utilizing it to produce aggregate statistics. Additionally, organizations must make sure that aggregate data does not allow for the identification of specific people and that it is not utilized for reasons that are inconsistent with those for which it was originally gathered.

**CANADA LAW**

Personal information collection, use, and disclosure are regulated by federal law in Canada. Orga nizations in the private sector that gather, use, or disclose personal information while conducting business are subject to the Personal Information Protection and Electronic Documents Act (PIPE DA). Organizations must seek consent, keep the use and disclosure of personal information to a minimum, and protect it from illegal access among other requirements imposed by PIPEDA.

Personal information collection, use, and disclosure are regulated by federal law in Canada. Orga nizations in the private sector that gather, use, or disclose personal information while conducting business are subject to the Personal Information Protection and Electronic Documents Act (PIPE DA). Organizations must seek consent, keep the use and disclosure of personal information to a minimum, and protect it from illegal access, disclosure or use among other requirements imposed by PIPEDA.

It is challenging to control this practice because PIPEDA does not expressly forbid the collection and selling of aggregate data. Nevertheless, the Office of the Privacy Commissioner of Canada has published guidelines on the use of aggregate data that state organizations must ensure that individuals cannot be identified from the aggregate data and that they should obtain consent from individuals before using their personal information for this purpose. The guidelines advise

organizations to take steps to ensure that the data is accurate and current as well as to provide explanations of how they gather and utilize data that are simple to grasp.

However, there are some exceptions to these laws when it comes to using personal information in commercial purposes. One of these exceptions is the use of personal information for "business transactions." This refers to situations where personal information is necessary for carrying out a transaction that the individual concerned has already agreed to. For example, a business may need to disclose personal information to a payment processor to process a payment. In such cases, the disclosure of personal information is permissible without obtaining explicit consent from the individual concerned.

Another exception is the use of personal information for "marketing purposes." This exception allows businesses to use personal information for the purpose of marketing their products or services, but only if the individual has not explicitly opted out of such use. This means that businesses must obtain explicit consent before using personal information for marketing purposes, but they do not need to obtain explicit consent if the individual has not explicitly opted out.

# MORAL AND ETHICAL ANALYSIS

Although selling aggregate information and mining transaction data may legally be legal, there are various moral and ethical issues that must be considered.

The issue of consent comes first. It might be claimed that even if personal information is not disclosed, people have not formally authorized this use of their data. While it may be legal to utilize a person's personal information for marketing or business activities, it is less certain if doing so to create aggregate data that is then sold to third parties is legal.

The issue of transparency comes next. Businesses have a responsibility to disclose how they use customer information if they do. This implies that they must provide individuals with clear and understandable information about the acquisition, use, and disclosure of their personal information.

The issue of power dynamics comes up third. Large-scale personal data access gives corporations a great deal of power and sway over people. Companies can use this information to decide whether to provide a person credit or whether to target them with certain advertisements. This could lead to a power imbalance that isn't always in people's best interests.

Even though it might be lawful to mine transaction data and sell it to competitors as aggregate information, it raises ethical questions. This dilemma can be examined using the ACM/IEEE Code of Ethics for Software Engineers. Software engineers are required to "approach computer- related work with a full understanding of the relevant laws and regulations," as stated in the Code (ACM/IEEE, 2018, 1.4). To verify that the company's data mining and sharing methods are lawful and in compliance with applicable laws and regulations, a software engineer must first make sure that they are.

Software programmers must also "respect the privacy of others," according to the Code (ACM/IEEE, 2018, 3.7). Even though businesses may claim that they are just providing aggregate data rather than personal information, data aggregation can nevertheless result in the identification of specific people, especially when paired with other publicly available data. Software engineers must therefore make sure that the company's data mining and sharing activities do not jeopardize its customers' privacy.

Software programmers must "be fair and take steps not to discriminate," according to the Code (ACM/IEEE, 2018, 3.8). The company may be giving certain businesses an unfair edge over others by selling aggregate information to rivals, particularly smaller rivals who cannot afford to buy the aggregate information. Software engineers must therefore make sure that the organization's data mining and sharing processes do not prejudice any one enterprise.

**PRINCIPLE 1: PUBLIC**

The software engineering code of ethics' first principle is broken by the practice of selling clients' meta data. Software programmers are not operating in the public interest by doing this, nor are they taking user interests into account. Additionally, they are breaking the ethical rules of transpa rency and disclosure by not warning the clients about any potential risks associated with such an activity.

**PRINCIPLE 2: CLIENT AND EMPLOYER**

The software engineering code of ethic’s second principle is broken in the following ways:

* Use the property of a client or employer only in ways properly authorized: The web hosting company is using the transaction data of its clients' websites without properly authorizing it for this purpose. This violates the principle of using the property of a client or employer only in ways properly authorized.
* Keep private any confidential information gained in their professional work: The transaction data of the clients' websites is confidential information gained in the web hosting company's professional work. By selling this information, the company is not keeping it private, which violates this principle.
* Identify, document, collect evidence and report to the client or the employer promptly if, in their opinion, a project is likely to fail, to prove too expensive, to violate intellectual property law, or otherwise to be problematic: The web hosting company has not identified or reported the potential problems that may arise from collecting and selling the transaction data of its clients' websites. This violates the principle of identifying and reporting potential problems to the client or employer promptly.
* Accept no outside work detrimental to the work they perform for their primary employer: The web hosting company is engaging in outside work (i.e. selling transaction data to competing companies) that is detrimental to the work they perform for their primary employer (i.e. hosting websites). This violates the principle of accepting no outside work detrimental to the work they perform for their primary employer.

**PRINCIPLE 3: PRODUCT**

The principle 3 is broken when a company supplying WebHosting for ecommerce sites mines the transactions of the websites it is hosting and sells the aggregate information on traffic to competing companies without the explicit consent of the clients. This violates the ethical considerations of software engineering, especially with regards to the confidentiality and privacy of personal data. The clients trust the web hosting company to keep their transaction data secure and private, and the company is obligated to maintain that trust.

This practice would violate the principle of striving for high quality, acceptable cost, and reasonable schedules because the company is prioritizing its own financial gain over ensuring the privacy and security of its clients' data.

Furthermore, this activity may also be illegal and against data protection laws, depending on the jurisdiction. In many countries, the collection and sale of personal data without explicit consent is considered a violation of privacy rights, and the company could face legal repercussions.

Finally, this activity also violates the economic and cultural considerations of software engineering. It creates an unfair advantage for competing companies who can access valuable information without putting in the effort and resources to collect it themselves. This can lead to market distortions and a lack of fair competition, which can harm the overall economy.

Therefore, software engineers must ensure that their products and related modifications meet the highest professional standards possible, including ethical, legal, and economic considerations. They must strive for high quality and ensure that proper goals and objectives are identified, and that ethical, economic, cultural, legal, and environmental issues related to work projects are

addressed. They must follow professional standards and ensure that they are qualified for any project on which they work or propose to work.

**PRINCIPLE 4: JUDGEMENT**

It may be unethical to sell statistical data about website transactions to rival businesses, which violates Principle 4 of the Software Engineering Code of Ethics. It may be perceived as a dishonest financial practise, threaten professional neutrality, and go against the idea of revealing conflicts of interest. Customers rely on web hosts to preserve their privacy, so disclosing that information to rivals is not in their best interests. In conclusion, this approach violates the idea of retaining independence and integrity in professional judgement.

**PRINCIPLE 5: MANAGEMENT**

Software engineering managers must encourage an ethical approach to software development and maintenance, according to Principle 5 of the Software Engineering Code of Ethics. The company's regulations for protecting sensitive information are broken when aggregate information about customer transactions is mined and sold to rival businesses. This can also lure in staff under false pretenses. Encouraging software developers to take part in such activities is against the spirit of this Code and goes against the idea of encouraging moral conduct. This kind of behavior violates the company's policies and processes for preserving confidential information and does not support an ethical approach to software development and management, which is a violation of Principle 5.

**PRINCIPLE 6: PROFESSION**

Software Engineering Code of Ethics Principle 6 prohibits the mining and sale of proprietary knowledge. In the interest of the public, software developers have a duty to uphold the integrity and reputation of the industry. They go against this ideal by selling information for profit and deceive customers about the features of their software. Failure to disclose the transaction to clients also reveals a lack of adherence to the Code of Ethics. In conclusion, selling confidential information breaches software engineers' obligations to be accurate and truthful about their work, misleads clients, and compromises the profession's obligation to advance ethical behavior.

**PRINCIPLE 7: COLLEAGUES**

Software engineers should be fair to and supportive of their coworkers, according to Principle 7 of the Software Engineering Code of Conduct, which prohibits mining and selling confidential information about website transactions. This is because it undercuts the efforts of coworkers who oversee preserving sensitive information and puts them at risk of having their competency questioned. It also does not acknowledge the contributions of others and does not help colleagues stay informed about current best practices. The involved software engineers are treating their coworkers unfairly and failing to uphold their obligation to promote their professional development by breaking these values.

**PRINCIPLE 8: SELF**

There is a breach of Principle 8 of the Software Engineering Code of Ethics when competitors are given access to private information about website transactions through illegal data mining. This concept mandates that software engineers engage in lifelong learning and support a moral attitude to the profession. Software engineers are not improving their understanding of the relevant standards and rules regulating the software and related documents on which they work by engaging in the immoral act of selling sensitive information. Also, they are doing a poor job of enhancing their capacity to produce high-quality, secure, and useful software within appropriate cost and schedule constraints. The act of mining and selling confidential information can be seen as a personal violation of the Code, which is inconsistent with being a professional software engineer.

# CONCLUSION

In conclusion, Software engineers must adhere to the ideals and concepts of professionalism, responsibility, and accountability, which is why ethics is such an important part of the field. It offers recommendations to assist software engineers in making moral choices consistent with the standards of their profession. The safety, privacy, and security of the software's end users are given top priority by software engineers because of ethical considerations in the field.

Additionally, it aids in defending the rights of those whose interests may be impacted by the software, such as the public, clients, shareholders, and staff. In addition to ensuring that software engineers follow all applicable rules and regulations, ethics also serves to foster transparency and trust between software engineers, clients, and the general public. Ultimately, ethical considerations in software engineering help to promote the integrity and reputation of the profession and ensure that software engineers act responsibly and with the utmost professionalism.

.

# BIBLIOGRAPHY

ACM/IEEE. (2018). Software Engineering Code of Ethics and Professional Practice.

Retrieved from https://[www.acm.org/binaries/content/assets/standards/code-](http://www.acm.org/binaries/content/assets/standards/code-) of-ethics-booklet-fnl.pdf

British Columbia. (n.d.). Personal Information Protection Act. Queen’s Printer.

Retrieved from https://[www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063\_01](http://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/03063_01)

Canada. (2000). Personal Information Protection and Electronic Documents Act. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

Kshetri, N. (2014). Big data’s impact on privacy, security and consumer welfare. Telecommunications Policy, 38(4), 291-298. doi: 10.1016/j.telpol.2013.12.008

Murphy, K. (2017). Big data: ethical considerations. Journal of Social Work Practice, 31(2), 153-165. doi: 10.1080/02650533.2017.1283649

Office of the Privacy Commissioner of Canada. (2017). OPC’s guidance on inappropriate data practices: Interpretation and application of subsection 5(3). Retrieved from https://[www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-](http://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-) information-protection-and-electronic-documents-act-pipeda/pipeda-compliance- help/guidance-documents/inap\_2017/

Ontario. (n.d.). Freedom of Information and Protection of Privacy Act. Queen’s Printer. Retrieved from https://[www.ontario.ca/laws/statute/90f31](http://www.ontario.ca/laws/statute/90f31)

Professional Engineers and Geoscientists of British Columbia. (2019). Code of Ethics. Retrieved from https://[www.apeg.bc.ca/getmedia/85681c31-c9a7-41f3-9de3-](http://www.apeg.bc.ca/getmedia/85681c31-c9a7-41f3-9de3-) 3a7333f8f441/Code-of-Ethics-2019.aspx

The Association for Computing Machinery. (2018). ACM Code of Ethics and Professional Conduct. Retrieved from https://[www.acm.org/code-of-ethics](http://www.acm.org/code-of-ethics)

The Institute of Electrical and Electronics Engineers. (2020). IEEE Code of Ethics. Retrieved from https://[www.ieee.org/content/dam/ieee-](http://www.ieee.org/content/dam/ieee-) org/ieee/web/org/about/ieee\_code\_of\_ethics.pdf

The Law Society of British Columbia. (n.d.). Code of Professional Conduct for British Columbia. Retrieved from https://[www.lawsociety.bc.ca/support-and-resources-for-](http://www.lawsociety.bc.ca/support-and-resources-for-) lawyers/professional-regulation/the-code-of-professional-conduct-for-british-columbia/